MULLEN COUGHLIN LLC
ATTORNEYS AT LAW

James E. Prendergast
Office: 267-930-4798
Fax: 267-930-4771
Email: jprendergast@mullen.law

1275 Drummers Lane, Suite 302
Wayne, PA 19087

December 31, 2018

**INTENDED FOR ADDRESSEE(S) ONLY**

**VIA U.S. MAIL**

Attorney General Gordon J. MacDonald
Office of the New Hampshire Attorney General
Attn: Security Breach Notification
33 Capitol Street
Concord, NH 03301

**Re: Notice of Data Event**

Dear Sir or Madam:

We represent Aimbridge Hospitality Holdings, LLC headquartered at 5851 Legacy Circle, Suite 400, Plano, TX 75024. Aimbridge Hospitality Holdings, LLC is an independent hotel management company that owns certain entities under the Aimbridge Hospitality Holdings, LLC umbrella. We write to notify you, on behalf of certain entities owned by Aimbridge Hospitality Holdings, LLC, listed in ***Exhibit A***, of an event that may affect the security of personal information relating to one hundred thirty-five (135) New Hampshire residents. The investigation into this matter is ongoing, and this notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, Aimbridge Hospitality Holdings, LLC does not waive any rights or defenses regarding the applicability of New Hampshire law, the applicability of the New Hampshire data event notification statute, or personal jurisdiction.

**Nature of the Data Event**

On September 14, 2018, Aimbridge Hospitality Holdings, LLC became aware of unusual activity in an employee's email account. They immediately launched an investigation into the unusual activity. With the assistance of computer forensics experts, they learned of an email phishing incident which resulted in unauthorized access to a number of employees' email accounts between June 7, 2018 and September 24, 2018. After determining there was unauthorized access, they undertook a lengthy and labor-intensive process to identify the personal information contained within the affected email accounts. It could not be confirmed whether this information was actually accessed by an unauthorized individual(s). On November 28, 2018, the investigation confirmed that the information potentially subject to unauthorized access or acquisition related to New Hampshire residents. Although Aimbridge Hospitality Holdings, LLC is unaware of any actual or attempted misuse of the personal information, they notified the affected individuals in an abundance of caution because their information was present in the impacted email accounts.

The information that could have been subject to unauthorized access includes: name, Social Security number, financial account number and/or Driver's License number.

**Notice to New Hampshire Residents**

On or about December 31, 2018, the properties listed in ***Exhibit A***, began providing written notice of this incident to affected individuals, which includes one hundred thirty-five (135) New Hampshire resident(s). Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit B***.

**Other Steps Taken and To Be Taken**

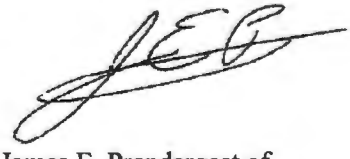
Upon discovering the event, Aimbridge Hospitality Holdings, LLC moved quickly to investigate and respond to the incident, assess the security of Aimbridge Hospitality Holdings, LLC systems, and notify potentially affected individuals. Aimbridge Hospitality Holdings, LLC reset passwords for all affected accounts, implemented multi-factor authentication for email access and enhanced email security, conducted additional employee training, and are currently reviewing our policies and procedures relating to data security.

While Aimbridge Hospitality Holdings, LLC are unaware of any actual or attempted misuse of the affected information, they are offering affected individuals one (1) year of complimentary credit monitoring and identity restoration services through TransUnion Interactive. Additionally, Aimbridge Hospitality Holdings, LLC is providing impacted individuals with guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud. Aimbridge Hospitality Holdings, LLC is also providing individuals with information on how to place a fraud alert and security freeze on one's credit file, information on protecting against tax fraud, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

**Contact Information**

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4798.

Very truly yours,



James E. Prendergast of
MULLEN COUGHLIN LLC

JEP:mal
Enclosure

# EXHIBIT A

| Company |
| --- |
| AH 2005 Management, L.P. |
| AH 2007 Management, L.P. |
| AHR Employee Service LLC |
| Aimbridge (PR) Services LLC |
| Aimbridge Employee Service Corp. |
| Aimbridge Hospitality, LLC |
| Aimbridge Management West, LLC |
| Channel Point Employee Service LLC |
| Evolution Hospitality, LLC |
| Hotel Recovery Management LLC |
| Marcus Clayton, LLC |
| Pillar Hotels and Resorts, LLC |
| Pillar Receiver, L.L.C. |
| TMI Employee Management, L.P. |
| Vindicare Hospitality LLC |
| Vindicare Management LLC |

# EXHIBIT B

<<Company Letterhead>>
Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

<<Mail ID>>
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<Address 5>>
<<City>><<State>><<Zip>>
<<Country>>

<<Date>>

**RE: Notice of Data Breach**

Dear <<Name 1>>:

<<Company>> is writing to notify you of an incident that may affect the security of your personal information. We are providing you with information regarding the incident, steps we have taken since discovering the incident, and what you can do to protect your personal information should you feel it is appropriate to do so.

***What Happened?*** On September 14, 2018, we became aware of unusual activity in an employee's email account. We immediately launched an internal investigation into the unusual activity. With the assistance of computer forensics experts, we learned <<Company>> was the victim of an email phishing incident which resulted in unauthorized access to a number of employees' email accounts between June 7, 2018 and September 24, 2018. After determining there was unauthorized access, we undertook a lengthy and labor-intensive process to identify the personal information contained within the affected email accounts. On November 28, 2018, our investigation confirmed the identity of the individuals whose personal information was affected. Based on available forensic evidence, an email containing your personal information was potentially subject to unauthorized access. Although we are unaware of any actual or attempted misuse of your personal information, we are notifying you in an abundance of caution because your information was present in the impacted email accounts.

***What Information Was Involved?*** We cannot confirm if your information was actually accessed by the unauthorized individual. However, our investigation confirmed the information present in the impacted email accounts includes your name, <<Data Elements>>.

***What We Are Doing.*** Information privacy and security are among our highest priorities. We have strict security measures in place to protect information in our care. Upon learning of this incident, we quickly took steps to confirm the security of our systems, including our employee email accounts. We reset passwords for the affected email accounts, implemented increased security measures for email account access, conducted additional employee training, and are currently reviewing our policies and procedures relating to data security. In an abundance of caution, we are also notifying potentially affected individuals, including you, so that you may take further steps to best protect your personal information, should you feel it is appropriate to do so.

Although we are not aware of any actual or attempted misuse of information as a result of this event, as a safeguard, we have arranged for you to enroll, at no cost to you, in an online credit monitoring service (*my*TrueIdentity) for <<Credit Monitoring Months>> months provided by TransUnion Interactive, a subsidiary of TransUnion®, one of the three nationwide credit reporting companies.

**How to Enroll: You can sign up online or via U.S. Mail delivery**

- To enroll in this service, go to the *my*TrueIdentity website at **www.MyTrueIdentity.com** and, in the space referenced as "Enter Activation Code," enter the 12-letter Activation Code **<<Insert Unique 12-letter Activation Code>>** and follow the three steps to receive your credit monitoring service online within minutes.

- If you do not have access to the Internet and wish to enroll in a similar offline, paper-based credit monitoring service, via U.S. Mail delivery, please call the TransUnion Fraud Response Services toll-free hotline at **1-855-288-5422**. When prompted, enter the six-digit telephone passcode **<<Insert static 6-digit Telephone Pass Code>>** and follow the steps to enroll in the offline credit monitoring service, add an initial fraud alert to your credit file, or to speak to a TransUnion representative if you believe you may be a victim of identity theft.

You can sign up for the online or offline credit monitoring service anytime between now and **<<Enrollment Deadline>>**. Due to privacy laws, we cannot register you directly. Please note that credit monitoring services might not be available for individuals who do not have a credit file with TransUnion or an address in the United States (or its territories) and a valid Social Security number. Enrolling in this service will not affect your credit score.

**ADDITIONAL DETAILS REGARDING YOUR <<Credit Monitoring Months>>-MONTH COMPLIMENTARY CREDIT MONITORING SERVICE:**

- Once you are enrolled, you will be able to obtain one year of unlimited access to your TransUnion credit report and credit score.
- The daily credit monitoring service will notify you if there are any critical changes to your credit file at TransUnion, including fraud alerts, new inquiries, new accounts, new public records, late payments, changes of address, and more.

The service also includes access to an identity restoration program that provides assistance in the event that your identity is compromised and up to $1,000,000 in identity theft insurance with no deductible. (Policy limitations and exclusions may apply.)

***What You Can Do.*** You may review the information contained in the attached "Steps You Can Take to Protect Against Identity Theft and Fraud." You may also enroll to receive the identity protection services we are making available to you. We will cover the cost of this service; however, you will need to enroll yourself in this service. Instructions on how to enroll and receive the complimentary monitoring and restoration services are above.

***For More Information.*** We understand that you may have questions about this incident that are not addressed in this letter. If so, you may contact our call center at 877-845-7486, which is available Monday through Friday from 9 A.M. to 9 P.M. Eastern Time.

We sincerely regret the inconvenience this incident causes for you. <<Company>> remains committed to safeguarding information in our care and will continue to take proactive steps to enhance data security.

Sincerely,

Gregory J Moundas

Gregory Moundas
Vice President
<<Company>>

Enclosure

## Steps You Can Take to Protect Against Identity Theft and Fraud

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity. Under U.S. law you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

You have the right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a security freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

| **Experian** | **TransUnion** | **Equifax** |
|---|---|---|
| PO Box 9554 | P.O. Box 2000 | PO Box 105788 |
| Allen, TX 75013 | Chester, PA 19016 | Atlanta, GA 30348-5788 |
| 1-888-397-3742 | 1-888-909-8872 | 1-800-685-1111 |
| www.experian.com/freeze/center.html | www.transunion.com/credit-freeze | www.equifax.com/personal/credit-report-services |

In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, military identification, etc.);
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

As an alternative to a security freeze, you have the right to place an initial or extended "fraud alert" on your file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the agencies listed below:

| **Experian** | **TransUnion** | **Equifax** |
|---|---|---|
| P.O. Box 2002 | P.O. Box 2000 | P.O. Box 105069 |
| Allen, TX 75013 | Chester, PA 19106 | Atlanta, GA 30348 |
| 1-888-397-3742 | 1-800-680-7289 | 1-888-766-0008 |
| www.experian.com/fraud/center.html | www.transunion.com/fraud-victim-resource/place-fraud-alert | www.equifax.com/personal/credit-report-services |

Although we have no reason to believe that your personal information has been used to file fraudulent tax returns, you can contact the IRS at www.irs.gov/Individuals/Identity-Protection for helpful information and guidance on steps you can take to address a fraudulent tax return filed in your name and what to do if you become the victim of such fraud. You can also visit www.irs.gov/uac/Taxpayer-Guide-to-Identity-Theft for more information.

You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself, by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General.

The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338); TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

**For North Carolina residents**, the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-566-7226 or 1-919-716-6400, www.ncdoj.gov.

**For Maryland residents**, the Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, 1-888-743-0023, www.oag.state.md.us.

**For New Mexico residents**, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

**For Rhode Island Residents:** The Rhode Island Attorney General can be reached at: 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, 1-401-247-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are 153 Rhode Island residents impacted by this incident.

<<Company Letterhead>>
Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

<<Mail ID>>
Parent/Guardian of
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<Address 5>>
<<City>><<State>><<Zip>>
<<Country>>

<<Date>>

**RE: Notice of Data Breach**

Dear Parent/Guardian of <<Name 1>>:

<<Company>> is writing to notify you of an incident that may affect the security of some of your dependent's personal information. We are providing you with information regarding the incident, steps we have taken since discovering the incident, and what you can do to protect this personal information should you feel it is appropriate to do so.

***What Happened?*** On September 14, 2018, we became aware of unusual activity in an employee's email account. We immediately launched an internal investigation into the unusual activity. With the assistance of computer forensics experts, we learned <<Company>> was the victim of an email phishing incident which resulted in unauthorized access to a number of employees' email accounts between June 7, 2018 and September 24, 2018. After determining there was unauthorized access, we undertook a lengthy and labor-intensive process to identify the personal information contained within the affected email accounts. On November 28, 2018, our investigation confirmed the identity of the individuals whose personal information was affected. Based on available forensic evidence, an email containing your dependent's personal information was potentially subject to unauthorized access. Although we are unaware of any actual or attempted misuse of this personal information, we are notifying you in an abundance of caution because this information was present in the impacted email accounts.

***What Information Was Involved?*** We cannot confirm if your dependent's information was actually accessed by the unauthorized individual. However, our investigation confirmed the information present in the impacted email accounts includes your dependent's name, <<Data Elements>>.

***What We Are Doing.*** Information privacy and security are among our highest priorities. We have strict security measures in place to protect information in our care. Upon learning of this incident, we quickly took steps to confirm the security of our systems, including our employee email accounts. We reset passwords for the affected email accounts, implemented increased security measures for email account access, conducted additional employee training, and are currently reviewing our policies and procedures relating to data security. In an abundance of caution, we are also notifying potentially affected individuals, including you, so that you may take further steps to best protect your dependent's personal information, should you feel it is appropriate to do so.

Although we are not aware of any actual or attempted misuse of information as a result of this event, as a safeguard, we have arranged for your dependent to enroll, at no cost to you, in an online credit monitoring service (*my*TrueIdentity) for <<Credit Monitoring Months>> months provided by TransUnion Interactive, a subsidiary of TransUnion®, one of the three nationwide credit reporting companies.

**How to Enroll: You can sign up online or via U.S. Mail delivery**

- To enroll in this service, go to the *my*TrueIdentity website at **www.MyTrueIdentity.com** and, in the space referenced as "Enter Activation Code," enter the 12-letter Activation Code **<<Insert Unique 12-letter Activation Code>>** and follow the three steps to receive your credit monitoring service online within minutes.
- If you do not have access to the Internet and wish to enroll in a similar offline, paper-based credit monitoring service, via U.S. Mail delivery, please call the TransUnion Fraud Response Services toll-free hotline at **1-855-288-5422**. When prompted, enter the six-digit telephone passcode **<<Insert static 6-digit Telephone Pass Code>>** and follow the steps to enroll in the offline credit monitoring service, add an initial fraud alert to your credit file, or to speak to a TransUnion representative if you believe you may be a victim of identity theft.

You can sign up for the online or offline credit monitoring service anytime between now and **<<Enrollment Deadline>>**. Due to privacy laws, we cannot register you directly. Please note that credit monitoring services might not be available for individuals who do not have a credit file with TransUnion or an address in the United States (or its territories) and a valid Social Security number. Enrolling in this service will not affect your credit score.

**ADDITIONAL DETAILS REGARDING YOUR <<Credit Monitoring Months>>-MONTH COMPLIMENTARY CREDIT MONITORING SERVICE:**

- Once you are enrolled, you will be able to obtain one year of unlimited access to your TransUnion credit report and credit score.
- The daily credit monitoring service will notify you if there are any critical changes to your credit file at TransUnion, including fraud alerts, new inquiries, new accounts, new public records, late payments, changes of address, and more.

The service also includes access to an identity restoration program that provides assistance in the event that your identity is compromised and up to $1,000,000 in identity theft insurance with no deductible. (Policy limitations and exclusions may apply.)

**Special note for minors affected by this incident:** The same services referred to above may not be available to affected minors. As an alternative, parents/legal guardians can check to see if your child may be a victim of identity theft by using TransUnion's secure online form at www.transunion.com/childidentitytheft to submit your information so TransUnion can check their database for a credit file with your child's Social Security Number. After TransUnion's search is complete, they will respond to you at the email address you provide. If they locate a file in your child's name, they will ask you for additional information in order to proceed with steps to protect your child from any impact associated with this fraudulent activity.

***What You Can Do.*** You may review the information contained in the attached "Steps You Can Take to Protect Against Identity Theft and Fraud." You may also enroll to receive the identity protection services we are making available to you. We will cover the cost of this service; however, you will need to enroll your dependent in this service. Instructions on how to enroll are above.

***For More Information.*** We understand that you may have questions about this incident that are not addressed in this letter. If so, you may contact our call center at 877-845-7486, which is available Monday through Friday from 9 A.M. to 9 P.M. Eastern Time.

We sincerely regret the inconvenience this incident causes for you. <<Company>> remains committed to safeguarding information in our care and will continue to take proactive steps to enhance data security.

Sincerely,

Gregory J Moundas

Gregory Moundas
Vice President
<<Company>>

Enclosure

## Steps You Can Take to Protect Against Identity Theft and Fraud

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your dependent's account statements, and to monitor credit reports for suspicious activity. Under U.S. law you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

You have the right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a security freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

| **Experian** | **TransUnion** | **Equifax** |
|---|---|---|
| PO Box 9554 | P.O. Box 2000 | PO Box 105788 |
| Allen, TX 75013 | Chester, PA 19016 | Atlanta, GA 30348-5788 |
| 1-888-397-3742 | 1-888-909-8872 | 1-800-685-1111 |
| www.experian.com/freeze/center.html | www.transunion.com/credit-freeze | www.equifax.com/personal/credit-report-services |

In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, military identification, etc.);
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

As an alternative to a security freeze, you have the right to place an initial or extended "fraud alert" on your file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the agencies listed below:

| **Experian** | **TransUnion** | **Equifax** |
|---|---|---|
| P.O. Box 2002 | P.O. Box 2000 | P.O. Box 105069 |
| Allen, TX 75013 | Chester, PA 19106 | Atlanta, GA 30348 |
| 1-888-397-3742 | 1-800-680-7289 | 1-888-766-0008 |
| www.experian.com/fraud/center.html | www.transunion.com/fraud-victim-resource/place-fraud-alert | www.equifax.com/personal/credit-report-services |

Although we have no reason to believe that your dependent's personal information has been used to file fraudulent tax returns, you can contact the IRS at www.irs.gov/Individuals/Identity-Protection for helpful information and guidance on steps you can take to address a fraudulent tax return filed in your name and what to do if you become the victim of such fraud. You can also visit www.irs.gov/uac/Taxpayer-Guide-to-Identity-Theft for more information.

You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself, by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General.

The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338); TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

**For North Carolina residents**, the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-566-7226 or 1-919-716-6400, www.ncdoj.gov.

**For Maryland residents**, the Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, 1-888-743-0023, www.oag.state.md.us.

**For New Mexico residents**, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

**For Rhode Island Residents:** The Rhode Island Attorney General can be reached at: 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, 1-401-247-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are 153 Rhode Island residents impacted by this incident.

<<Company Letterhead>>
Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

<<Mail ID>>
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<Address 5>>
<<City>><<State>><<Zip>>
<<Country>>

<<Date>>

**RE: Notice of Data Breach**

Dear <<Name 1>>:

<<Company>> is writing to notify you of an incident that may affect the security of your personal information. We are providing you with information regarding the incident, steps we have taken since discovering the incident, and what you can do to protect your personal information should you feel it is appropriate to do so.

***What Happened?*** On September 14, 2018, we became aware of unusual activity in an employee's email account. We immediately launched an internal investigation into the unusual activity. With the assistance of computer forensics experts, we learned <<Company>> was the victim of an email phishing incident which resulted in unauthorized access to a number of employees' email accounts between June 7, 2018 and September 24, 2018. After determining there was unauthorized access, we undertook a lengthy and labor-intensive process to identify the personal information contained within the affected email accounts. On November 28, 2018, our investigation confirmed the identity of the individuals whose personal information was affected. Based on available forensic evidence, an email containing your personal information was potentially subject to unauthorized access again. This information consisted of the same information previously exposed earlier this year during a similar event, for which you have already been notified. Our forensic experts have assessed that the current event was likely perpetrated by the same criminal enterprise as the previous matter. Although we are still unaware of any actual or attempted misuse of your personal information, we are notifying you again in an abundance of caution because your information was present in the recently impacted email accounts.

***What Information Was Involved?*** We still cannot confirm if your information was actually accessed by the unauthorized individual. However, our investigation confirmed the information present in the impacted email accounts includes your name, <<Data Elements>>.

***What We Are Doing.*** Information privacy and security are among our highest priorities. We have strict security measures in place to protect information in our care. Upon learning of this incident, we quickly took steps to confirm the security of our systems, including our employee email accounts. We reset passwords for the affected email accounts, implemented increased security measures for email account access, conducted additional employee training, and are currently reviewing our policies and procedures relating to data security. In an abundance of caution, we are also notifying potentially affected individuals, including you, so that you may take further steps to best protect your personal information, should you feel it is appropriate to do so.

Although we are not aware of any actual or attempted misuse of information as a result of this event, as a safeguard, we have arranged for you to enroll, at no cost to you, in an online credit monitoring service (*my*TrueIdentity) for <<Credit Monitoring Months>> months provided by TransUnion Interactive, a subsidiary of TransUnion®, one of the three nationwide credit reporting companies.

**How to Enroll: You can sign up online or via U.S. Mail delivery**

- To enroll in this service, go to the *my*TrueIdentity website at **www.MyTrueIdentity.com** and, in the space referenced as "Enter Activation Code," enter the 12-letter Activation Code **<<Insert Unique 12-letter Activation Code>>** and follow the three steps to receive your credit monitoring service online within minutes.
- If you do not have access to the Internet and wish to enroll in a similar offline, paper-based credit monitoring service, via U.S. Mail delivery, please call the TransUnion Fraud Response Services toll-free hotline at **1-855-288-5422**. When prompted, enter the six-digit telephone passcode **<<Insert static 6-digit Telephone Pass Code>>** and follow the steps to enroll in the offline credit monitoring service, add an initial fraud alert to your credit file, or to speak to a TransUnion representative if you believe you may be a victim of identity theft.

You can sign up for the online or offline credit monitoring service anytime between now and **<<Enrollment Deadline>>.** Due to privacy laws, we cannot register you directly. Please note that credit monitoring services might not be available for individuals who do not have a credit file with TransUnion or an address in the United States (or its territories) and a valid Social Security number. Enrolling in this service will not affect your credit score.

**ADDITIONAL DETAILS REGARDING YOUR <<Credit Monitoring Months>>-MONTH COMPLIMENTARY CREDIT MONITORING SERVICE:**

- Once you are enrolled, you will be able to obtain one year of unlimited access to your TransUnion credit report and credit score.
- The daily credit monitoring service will notify you if there are any critical changes to your credit file at TransUnion, including fraud alerts, new inquiries, new accounts, new public records, late payments, changes of address, and more.

The service also includes access to an identity restoration program that provides assistance in the event that your identity is compromised and up to $1,000,000 in identity theft insurance with no deductible. (Policy limitations and exclusions may apply.)

***What You Can Do.*** You may review the information contained in the attached "Steps You Can Take to Protect Against Identity Theft and Fraud." You may also enroll to receive the identity protection services we are making available to you. We will cover the cost of this service; however, you will need to enroll yourself in this service. If you have previously enrolled in credit monitoring from our prior notification, the additional <<Credit Monitoring Months>> months of credit monitoring will be extended from the end of your current monitoring period, at no cost to you. Instructions on how to enroll and receive the complimentary monitoring and restoration services are above.

***For More Information.*** We understand that you may have questions about this incident that are not addressed in this letter. If so, you may contact our call center 877-845-7486, which is available Monday through Friday from 9 A.M. to 9 P.M. Eastern Time.

We sincerely regret the inconvenience this incident causes for you. <<Company>> remains committed to safeguarding information in our care and will continue to take proactive steps to enhance data security.

Sincerely,

Gregory Moundas
Vice President
<<Company>>

Enclosure

## Steps You Can Take to Protect Against Identity Theft and Fraud

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity. Under U.S. law you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

You have the right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a security freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

| **Experian** | **TransUnion** | **Equifax** |
|---|---|---|
| PO Box 9554 | P.O. Box 2000 | PO Box 105788 |
| Allen, TX 75013 | Chester, PA 19016 | Atlanta, GA 30348-5788 |
| 1-888-397-3742 | 1-888-909-8872 | 1-800-685-1111 |
| www.experian.com/freeze/center.html | www.transunion.com/credit-freeze | www.equifax.com/personal/credit-report-services |

In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, military identification, etc.);
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

As an alternative to a security freeze, you have the right to place an initial or extended "fraud alert" on your file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the agencies listed below:

| **Experian** | **TransUnion** | **Equifax** |
|---|---|---|
| P.O. Box 2002 | P.O. Box 2000 | P.O. Box 105069 |
| Allen, TX 75013 | Chester, PA 19106 | Atlanta, GA 30348 |
| 1-888-397-3742 | 1-800-680-7289 | 1-888-766-0008 |
| www.experian.com/fraud/center.html | www.transunion.com/fraud-victim-resource/place-fraud-alert | www.equifax.com/personal/credit-report-services |

Although we have no reason to believe that your personal information has been used to file fraudulent tax returns, you can contact the IRS at www.irs.gov/Individuals/Identity-Protection for helpful information and guidance on steps you can take to address a fraudulent tax return filed in your name and what to do if you become the victim of such fraud. You can also visit www.irs.gov/uac/Taxpayer-Guide-to-Identity-Theft for more information.

You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself, by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General.

The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338); TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

**For North Carolina residents**, the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-566-7226 or 1-919-716-6400, www.ncdoj.gov.

**For Maryland residents**, the Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, 1-888-743-0023, www.oag.state.md.us.

**For New Mexico residents**, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

**For Rhode Island Residents:** The Rhode Island Attorney General can be reached at: 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, 1-401-247-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are 153 Rhode Island residents impacted by this incident.